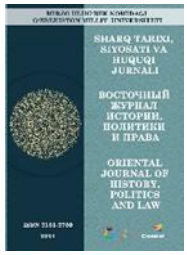
DOI: https://doi.org/10.37547/supsci-ojhpl-06-11-38 Pages: 443-458

Oriental Journal of History, Politics and Law

ORIENTAL JOURNAL OF HISTORY, POLITICS AND LAW

journal homepage:
https://www.supportscience.uz/index.php/ojhpl



CIVIL LAW ISSUES OF THE REGULATION OF ELECTRONIC PAYMENT SYSTEMS: ALLOCATION OF THE RISK OF UNAUTHORISED PAYMENTS

Nurzhakhan Erkinbaeva
PhD candidate
Tashkent State University of Law
E-mail: nurjakhanerkinbaeva@gmail.com
Tashkent, Uzbekistan

ABOUT ARTICLE

Key words: electronic payment system, payment service, electronic money, unauthorised payment, payment service provider liability, burden of proof, social engineering, civil law regulation.

Received: 09.11.2026
Accepted: 10.11.2026
Published: 11.11.2026

Abstract: The article examines the civil law aspects of the regulation of electronic payment systems in Uzbekistan, focusing on how the risk of unauthorised payments is allocated between the user and the payment service provider. The study analyses the Law "On Payments and Payment Systems", the Civil Code rules on settlements, the 2026 legislation on payment organisations and cybersecurity, and compares them with the law of Russia, Kazakhstan and the European Union (PSD2, the PSD3/PSR agreement of 2025 and the CJEU judgment in case C-70/25). Formal legal, comparative and modelling methods are used. The author shows that the specific rules on reimbursement and refund deadlines cover only bank cards, that the cardholder bears all risks until notifying the issuer, and that the burden of proving authorisation is not allocated. A risk allocation model is proposed for all payment instruments: a presumption of provider liability, a fixed cap on user losses expressed in base calculation units, refund by the next business day, release of the user where multi-factor authentication was not applied, and rules on transfers made by the user under deception. Provisions on a payment services contract in the Civil Code are also proposed.

ELEKTRON TO‘LOV TIZIMLARINI HUQUQIY TARTIBGA SOLISHNING FUQAROLIK-HUQUQIY MASALALARI: RUXSAT ETILMAGAN TO‘LOVLAR XAVFINI TAQSIMLASH

Nurjahon Erkinbayeva
Tayanch doktorant (PhD)
Toshkent davlat yuridik universiteti
E-mail: nurjakhanerkinbaeva@gmail.com
Toshkent, O‘zbekiston

MAQOLA HAQIDA

Kalit so‘zlar: elektron to‘lov tizimi, to‘lov xizmati, elektron pul, ruxsat etilmagan to‘lov, to‘lov xizmatlari yetkazib beruvchisining javobgarligi, isbotlash yuki, ijtimoiy muhandislik, fuqarolik-huquqiy tartibga solish.

Annotatsiya: Maqolada O‘zbekiston Respublikasida elektron to‘lov tizimlarini tartibga solishning fuqarolik-huquqiy jihatlari ruxsat etilmagan to‘lovlar xavfini foydalanuvchi va to‘lov xizmatlari yetkazib beruvchisi o‘rtasida taqsimlash masalasi misolida o‘rganilgan. «To‘lovlar va to‘lov tizimlari to‘g‘risida»gi Qonun, Fuqarolik kodeksining hisob-kitoblarga oid normalari, to‘lov tashkilotlari va kiberxavfsizlikka doir 2026-yilgi qonunchilik tahlil qilinib, Rossiya, Qozog‘iston va Yevropa Ittifoqi huquqi (PSD2, 2025-yilgi PSD3/PSR kelishuvi, Yevropa Ittifoqi Sudining C-70/25 ishi bo‘yicha qarori) bilan qiyoslangan. Formal-yuridik, qiyosiy-huquqiy va huquqiy modellashtirish usullari qo‘llanilgan. Muallif to‘lovni qoplash va qaytarish muddatlariga oid maxsus qoidalar faqat bank kartasiga taalluqli ekanini, karta egasi emitentni xabardor qilgunga qadar barcha xavfni o‘zi zimmasiga olishini hamda avtorizatsiyani isbotlash yuki taqsimlanmaganini ko‘rsatgan. Barcha to‘lov vositalari uchun xavfni taqsimlash modeli taklif etilgan: yetkazib beruvchi javobgarligi prezumpsiyasi, foydalanuvchi zararining bazaviy hisoblash miqdorida ifodalangan qat’iy chegarasi, mablag‘ni keyingi ish kunidan kechiktirmay qaytarish, ko‘p omilli autentifikatsiya qo‘llanilmagan hollarda foydalanuvchini zarardan ozod qilish va aldov ta’sirida amalga oshirilgan o‘tkazmalarga oid qoidalar. Shuningdek, Fuqarolik kodeksiga to‘lov xizmatlarini ko‘rsatish shartnomasi to‘g‘risidagi qoidalarni kiritish taklif qilingan.

ГРАЖДАНСКО-ПРАВОВЫЕ ВОПРОСЫ РЕГУЛИРОВАНИЯ ЭЛЕКТРОННЫХ ПЛАТЕЖНЫХ СИСТЕМ: РАСПРЕДЕЛЕНИЕ РИСКА НЕСАНКЦИОНИРОВАННЫХ ПЛАТЕЖЕЙ

Нуржахан Еркинбаева
Докторант (PhD)
Ташкентский государственный юридический университет
E-mail: nurjakhanerkinbaeva@gmail.com
Ташкент, Узбекистан

О СТАТЬЕ

Ключевые слова: электронная платежная система, платежная услуга, электронные деньги, несанкционированный платеж, ответственность поставщика платежных услуг, бремя доказывания, социальная инженерия, гражданско-правовое регулирование.

Аннотация: В статье рассмотрены гражданско-правовые аспекты регулирования электронных платежных систем в Республике Узбекистан на примере распределения риска несанкционированных платежей между пользователем и поставщиком платежных услуг. Проанализированы Закон «О платежах и платежных системах», нормы Гражданского кодекса о расчетах, законодательство 2026 г. о платежных организациях и кибербезопасности; они сопоставлены с правом России, Казахстана и Европейского союза (PSD2, соглашение 2025 г. по пакету PSD3/PSR, решение Суда ЕС по делу C-70/25). Использованы формально-юридический, сравнительно-правовой методы и метод правового моделирования. Показано, что специальные правила о возмещении и сроках возврата средств распространяются только на банковскую карту, до уведомления эмитента все риски несет держатель, а бремя доказывания авторизации не распределено. Предложена модель распределения риска для всех платежных инструментов: презумпция ответственности поставщика, фиксированный предел убытков пользователя в базовых расчетных величинах, возврат средств не позднее следующего рабочего дня, освобождение пользователя от убытков при неприменении многофакторной аутентификации и правила о переводах, совершенных клиентом под влиянием обмана. Обосновано включение в Гражданский кодекс положений о договоре об оказании платежных услуг.

Введение. Цифровизация расчетов отнесена к приоритетам государственной политики Республики Узбекистан: развитие безналичных платежей и финансовых технологий предусмотрено Стратегией «Цифровой Узбекистан – 2030» [1]. Рост рынка хорошо виден по данным Центрального банка: на 1 января 2026 г. в обращении находилось

более 68,27 млн банковских карт, а объем платежей через платежные терминалы за 2025 г. составил 460,25 трлн сумов против 326,7 трлн сумов годом ранее [2]. В обзоре платежных организаций, подготовленном KPMG по заказу и при информационной поддержке Центрального банка, объем безналичных расчетов по картам оценивается примерно в 72 % ВВП в 2025 г. (около 25 % в 2021 г.); через платежные организации за 2025 г. прошло порядка 412 трлн сумов, через мобильные приложения банков – около 646 трлн сумов [3].

Вместе с объемом операций растет и число несанкционированных платежей: хищений с использованием реквизитов карт, захвата учетных записей в мобильных приложениях, а также переводов, которые клиент совершает сам под влиянием обмана (так называемая социальная инженерия). В 2026 г. законодатель дважды обращался к этой проблеме. В апреле Сенат Олий Мажлиса одобрил закон о внесении изменений и дополнений в ряд законодательных актов, направленных на совершенствование деятельности операторов платежных систем и платежных организаций; закон предусматривает внедрение систем антифрода и биометрической идентификации и ставит задачу эффективной защиты прав потребителей платежных услуг [4]. В июле Законодательная палата приняла во втором чтении законопроект о совершенствовании обеспечения кибербезопасности и противодействия правонарушениям в цифровой среде, которым на банки, операторов платежных систем и платежные организации возлагается обязанность возмещать гражданам материальный ущерб, причиненный в результате несоблюдения требований кибербезопасности или непредотвращения мошеннических операций [5].

В отечественной литературе регулирование электронных платежных систем рассматривается главным образом с позиций банковского и финансового права: лицензирования, надзора, требований к капиталу и информационной безопасности. Частноправовые вопросы разработаны слабее. Неясно, какова правовая природа отношений пользователя с поставщиком платежных услуг, кто и по каким основаниям несет риск несанкционированного платежа, как распределяется бремя доказывания и каковы пределы ответственности сторон.

Цель статьи – определить гражданско-правовую модель распределения риска несанкционированных платежей в электронных платежных системах Республики Узбекистан и обосновать предложения по совершенствованию законодательства. Для ее достижения поставлены три исследовательских вопроса: 1) какова гражданско-правовая природа связей, образующих платежную систему, и прав пользователя на безналичные средства и электронные деньги; 2) как действующее законодательство Узбекистана распределяет риск несанкционированного платежа в сравнении с правом Российской

Федерации, Республики Казахстан и Европейского союза; 3) какие правила следует закрепить в Законе «О платежах и платежных системах» и Гражданском кодексе, чтобы распределение риска было предсказуемым для обеих сторон.

Обзор литературы. Теоретическую основу работы составляют исследования безналичных расчетов и денежных обязательств. Л.А. Новоселова обосновала взгляд на безналичные денежные средства как на обязательственные права требования клиента к банку [6]; близкие позиции развиты в работах Л.Г. Ефимовой о банковских сделках [7] и В.А. Белова о денежных обязательствах [8]. Для понимания платежа как цепочки обязательств между посредниками важна сравнительная работа Б. Гевы, в которой расчеты через банковскую систему рассматриваются как последовательность связанных распоряжений и исполнений [9].

Узбекистанская литература о платежном праве начала формироваться после принятия Закона «О платежах и платежных системах» 2019 г. Н. АллахРакха дал общий правовой анализ закона и его соотношения с международными стандартами [10]. У. Тухтаев рассмотрел проблемы регулирования электронных платежей в Республике Узбекистан, обращая внимание на необходимость защиты пользователей [11]. Ж. Эрполат исследовал гражданско-правовую ответственность за неисполнение обязательств при оказании платежных услуг и пришел к выводу, что ст. 795 Гражданского кодекса об ответственности банка за ненадлежащее совершение расчетных операций не отвечает условиям цифровых расчетов и нуждается в пересмотре [12]. В этих работах, однако, вопрос о распределении риска несанкционированной операции между пользователем и поставщиком специально не исследовался.

В зарубежной литературе последних лет внимание сместилось к мошенничеству, при котором платеж формально авторизует сам клиент (authorised push payment fraud). Группа европейских авторов под руководством Э. ван Праага проанализировала проект Регламента о платежных услугах (PSR) и предложила критерии распределения убытков от такого мошенничества между клиентом и поставщиком, включая учет превентивных обязанностей поставщика [13]. Этот подход используется в настоящей статье при построении авторской модели.

Методология исследования. Нормативную базу составили Гражданский кодекс Республики Узбекистан [14], Закон «О платежах и платежных системах» [15], законодательные акты 2026 г. о платежных системах и кибербезопасности [4; 5]. Для сравнения привлечены Федеральный закон Российской Федерации «О национальной платежной системе» [16], Закон Республики Казахстан «О платежах и платежных системах» [17], Директива (ЕС) 2015/2366 о платежных услугах (PSD2) [18], Директива

2009/110/EC об электронных деньгах (EMD2) [19], материалы политического соглашения по пакету PSD3/PSR [20] и практика Суда ЕС [21]. Статистические сведения о платежном рынке взяты из публикаций, основанных на данных Центрального банка [2; 3].

Использованы формально-юридический метод (толкование понятий и норм), сравнительно-правовой метод (сопоставление моделей распределения риска в четырех правопорядках), системный анализ (соотношение специального закона и Гражданского кодекса) и метод правового моделирования, с помощью которого построена предлагаемая схема распределения риска. Исследование носит теоретико-прикладной характер. Его ограничения связаны с тем, что опубликованная судебная практика Узбекистана по спорам о несанкционированных платежах немногочисленна, а законопроект о кибербезопасности на момент подготовки статьи не вступил в силу; поэтому выводы о его применении имеют прогностический характер. Эмпирические данные о числе и сумме мошеннических операций в Узбекистане в открытом доступе в систематизированном виде не публикуются и в работе не использовались.

Новизна исследования состоит в том, что риск несанкционированного платежа рассмотрен как предмет гражданско-правового распределения, а не только как вопрос надзорных требований к информационной безопасности; выявлено расхождение между правилом ст. 37 Закона, возлагающим на держателя карты все риски до уведомления эмитента, и общей конструкцией ответственности предпринимателя по Гражданскому кодексу; предложена многоуровневая модель распределения риска для всех платежных инструментов, включая операции, совершенные клиентом под влиянием обмана.

Результаты. *Платежная система как совокупность гражданско-правовых связей.* Закон «О платежах и платежных системах» определяет платежную систему как совокупность отношений, обеспечивающих осуществление платежей посредством взаимодействия оператора, участников и (или) платежных организаций с использованием процедур, инфраструктуры и правил, установленных оператором (ст. 5), а платежную организацию – как юридическое лицо, не являющееся банком, которое правомочно оказывать платежные услуги (ст. 4) [15]. Из этих определений следует, что платежная система не является субъектом права. Это сеть договоров, связывающих оператора с участниками, участников между собой и каждого поставщика платежных услуг с его клиентами.

В этой сети следует различать два уровня. Внутрисистемный уровень образуют договоры оператора с участниками, содержание которых определяется правилами платежной системы. Статья 8 Закона требует, чтобы правила описывали порядок функционирования системы, услуги, условия участия, процедуру отзыва распоряжения по

платежу и требования к защите информации; правила публикуются на сайте оператора и применяются через пятнадцать дней после опубликования [15]. По своей природе такие правила ближе к стандартным условиям договора присоединения, чем к нормативному акту. Клиентский уровень образуют договоры поставщика (банка или платежной организации) с пользователем: договор банковского счета, договор о выпуске и обслуживании карты, договор об использовании электронного кошелька, пользовательское соглашение мобильного приложения.

Основной гражданско-правовой конфликт возникает на клиентском уровне. Пользователь не является стороной правил платежной системы и не влияет на их содержание, однако условия о распределении риска мошеннических операций фактически определяются этими правилами и стандартными условиями поставщика. Гражданский кодекс не содержит специальной договорной конструкции для платежных услуг небанковских организаций: положения о банковском счете и расчетах рассчитаны на банк, а общие нормы о возмездном оказании услуг не учитывают, что услуга состоит в исполнении денежного обязательства через цепочку посредников [12; 14].

Электронные деньги и безналичные средства. Закон определяет электронные деньги как безусловные и безотзывные денежные обязательства эмитента, хранящиеся в электронной форме и принимаемые в качестве средства платежа (ст. 4) [15]. Этот подход близок к европейскому, где электронные деньги понимаются как денежная стоимость, представляющая собой требование к эмитенту и выпускаемая против получения денежных средств (ст. 2 EMD2) [19]. Владелец электронных денег, следовательно, имеет не вещь, а право требования к эмитенту, сходное с правом клиента на остаток по банковскому счету. Такая квалификация совпадает с позицией доктрины о безналичных деньгах как обязательственных правах [6–8].

Практическое следствие этого вывода состоит в следующем. Если распоряжение о списании не исходило от управомоченного лица, обязательство эмитента (банка) перед клиентом не прекращается надлежащим исполнением, поскольку исполнение произведено ненадлежащему лицу. По общему правилу риск такой операции лежит на поставщике. Закон подтверждает эту логику: согласно ст. 51 платеж является несанкционированным, если он осуществлен без соблюдения установленных требований или с использованием поддельных платежных инструментов, а ст. 52 предусматривает возврат средств по несанкционированным и ошибочным платежам, в том числе за счет участника, допустившего такой платеж [15].

Распределение риска в действующем законодательстве Узбекистана. Наиболее конкретные правила содержит ст. 37 «Несанкционированное использование банковской

карты». Эмитент обязан обеспечить круглосуточный прием сообщений об утрате карты или ее использовании без согласия держателя и немедленно блокировать карту; за операции после уведомления отвечает эмитент. Если же держатель не уведомил эмитента, все риски несет держатель. Держатель вправе обратиться за возмещением; заявление рассматривается в сроки, установленные ч. 7 ст. 36 (15 дней с возможным продлением до 30 дней, по операциям за пределами республики – до 45 дней), а при положительном решении средства зачисляются не позднее одного дня. Отказ допускается, если держатель не соблюдал предусмотренные договором меры безопасности или установлено его участие в преступлении с использованием карты [15].

Статья 53 возлагает на операторов и поставщиков обязанность применять многофакторную аутентификацию распоряжений, передаваемых по каналам удаленного доступа, вести журналы операций и шифровать данные; ст. 54 обязывает пользователя использовать платежный инструмент в соответствии с условиями и незамедлительно сообщать о его утрате или несанкционированном использовании. Статья 56 устанавливает, что инициатор платежа отвечает за убытки от несанкционированных платежей, если они возникли вследствие его мошенничества или необеспечения защиты средств идентификации, а ст. 58 предусматривает пеню в размере 0,1 % от суммы за каждый день просрочки платежа, но не более 10 % [15].

Сопоставление этих норм позволяет выделить несколько пробелов. Правило о распределении риска до уведомления и сроки возмещения установлены только для банковской карты; для электронных кошельков, переводов по номеру телефона, QR-платежей и операций в мобильных приложениях единых критериев нет. Бремя доказывания факта авторизации операции законом специально не распределено. Предельный размер убытков пользователя не установлен, а риск до уведомления возлагается на держателя полностью, независимо от того, мог ли он узнать о хищении реквизитов. Нарушение поставщиком обязанности применять многофакторную аутентификацию (ст. 53) прямо не связано с последствием в виде освобождения пользователя от убытков.

Сравнительно-правовой анализ. Зарубежные правопорядки решают эти вопросы непосредственно в законе (табл. 1).

Таблица 1. Распределение риска несанкционированного платежа: сравнительная характеристика

Критерий	Республика Узбекистан	Российская Федерация	Европейский союз
Основной источник	ЗРУ-578 (ст. 36, 37, 51–54, 56, 58); правила платежных систем	161-ФЗ (ст. 8, 9) в ред. 369-ФЗ	PSD2 (ст. 69–74); пакет PSD3/PSR (политическое соглашение 27.11.2025)
Сфера специальных правил	Ст. 37 – банковская карта; ст. 51–52 – общие понятия и возврат средств	Все электронные средства платежа	Все платежные инструменты
Бремя доказывания авторизации	Специально не распределено	Оператор возмещает операцию, если не исполнил обязанность информировать клиента	На поставщике (ст. 72 PSD2)
Риск до уведомления поставщика	Все риски несет держатель карты (ст. 37)	Клиент, если оператор надлежаще информировал его об операции	Не более 50 евро, кроме мошенничества и грубой неосторожности (ст. 74)
Риск после уведомления	Эмитент (ст. 37)	Оператор (ст. 9)	Поставщик (ст. 74)
Срок возврата средств	Рассмотрение заявления 15 дней (продление до 30, за рубежом до 45); зачисление не позднее 1 дня после решения	30 дней с даты заявления при переводе получателю из базы данных Банка России	Не позднее конца следующего рабочего дня (ст. 73)
Обман самого клиента	Законопроект 2026 г.: возмещение при несоблюдении требований кибербезопасности или непредотвращении мошеннических операций	С 25.07.2024: возмещение при переводе получателю из базы данных Банка России	PSR: сверка IBAN и имени получателя; ответственность поставщика при неисполнении превентивных обязанностей

Источник: составлено автором на основе [5; 15; 16; 18; 20–22].

В Европейском союзе Директива PSD2 возлагает на поставщика бремя доказывания того, что операция была аутентифицирована, правильно учтена и не затронута техническим сбоем (ст. 72), обязывает вернуть сумму несанкционированной операции не позднее конца следующего рабочего дня (ст. 73) и ограничивает убытки плательщика суммой 50 евро, кроме случаев мошенничества или умышленного либо грубо неосторожного нарушения им своих обязанностей (ст. 74) [18]. Если поставщик не требовал строгой аутентификации

клиента, плательщик не несет убытков, за исключением случаев мошенничества. Суд ЕС в решении от 15 октября 2026 г. по делу C-70/25 уточнил порядок применения этих норм: поставщик не вправе отказать в немедленном возврате средств лишь со ссылкой на грубую неосторожность клиента; отказ возможен только при обоснованном подозрении в мошенничестве, о котором поставщик письменно сообщает компетентному органу. Вопрос о том, должен ли клиент в итоге нести убытки, решается отдельно, и бремя доказывания его умысла или грубой неосторожности лежит на поставщике [21].

Политическое соглашение Совета ЕС и Европейского парламента от 27 ноября 2025 г. по пакету PSD3/PSR идет дальше. Перед переводом поставщик обязан сверять идентификатор счета с именем получателя; поставщики должны обмениваться информацией о мошенничестве; отдельно урегулировано мошенничество, при котором злоумышленник выдает себя за сотрудника поставщика; поставщик отвечает за убытки, если не исполнил обязанности по применению превентивных инструментов [20].

В Российской Федерации Закон «О национальной платежной системе» строится на обязанности оператора информировать клиента о каждой операции. Если оператор эту обязанность не исполнил, он возмещает сумму операции, совершенной без согласия клиента; после получения уведомления клиента об утрате электронного средства платежа или его использовании без согласия риск последующих операций также несет оператор (ст. 9) [16]. Федеральным законом от 24 июля 2023 г. № 369-ФЗ, вступившим в силу 25 июля 2024 г., введена обязанность оператора возместить клиенту в течение 30 дней средства, переведенные получателю, сведения о котором содержались в базе данных Банка России о случаях и попытках переводов без согласия клиента [22]. В Республике Казахстан в 2025 г. срок, на который финансовые организации вправе приостанавливать операции с признаками мошенничества, увеличен с трех до пяти рабочих дней [17; 23].

Во всех рассмотренных зарубежных правопорядках риск несанкционированной операции по общему правилу лежит на профессиональном участнике, а пользователь отвечает в пределах фиксированной суммы либо при доказанном умысле или грубой неосторожности. Законодательство Узбекистана развивается в том же направлении: законопроект 2026 г. прямо закрепляет обязанность банков, операторов и платежных организаций возмещать ущерб и вводит временное приостановление операций по банковским счетам, электронным кошелькам и криптоактивам в качестве меры процессуального принуждения [5]. При доработке законопроекта целесообразно уточнить, кто доказывает нарушение требований кибербезопасности: если это бремя возлагается на пользователя, он, не имея доступа к журналам аутентификации и антифрод-системам поставщика, фактически не сможет им воспользоваться.

Предлагаемая модель распределения риска. С учетом изложенного предлагается закрепить в Законе «О платежах и платежных системах» единые для всех платежных инструментов правила, представленные в табл. 2.

Таблица 2. Предлагаемая модель распределения риска несанкционированного платежа (авторская разработка)

Ситуация	Кто несет убытки	Предел для пользователя	Бремя доказывания	Срок возврата
Операция без участия пользователя до уведомления; правила безопасности не нарушены	Поставщик	Фиксированная сумма в БРВ	Поставщик доказывает аутентификацию и отсутствие сбоя	Не позднее следующего рабочего дня
Операция после уведомления поставщика	Поставщик	Не несет	Поставщик доказывает время получения уведомления	Не позднее следующего рабочего дня
Поставщик не применил многофакторную аутентификацию (ст. 53)	Поставщик	Не несет, кроме умысла	Поставщик доказывает применение аутентификации	Не позднее следующего рабочего дня
Грубая неосторожность пользователя (передача кода, PIN)	Пользователь	Без предела	Поставщик доказывает грубую неосторожность	Сначала возврат, затем требование к пользователю
Умысел или мошенничество пользователя	Пользователь	Без предела	Поставщик доказывает умысел	Возврат может быть приостановлен с письменным обоснованием и сообщением в Центральный банк
Перевод клиентом под влиянием обмана; поставщик не выполнил превентивные меры	Поставщик (при грубой неосторожности клиента – обе стороны соразмерно)	По усмотрению суда при долевом распределении	Клиент доказывает обман; поставщик – исполнение превентивных мер	Рассмотрение заявления в рабочих днях, установленных законом
Перевод клиентом под влиянием обмана; превентивные меры выполнены	Пользователь (с требованием к получателю о возврате неосновательного обогащения)	Без предела	Поставщик доказывает исполнение мер	Не применяется

Модель исходит из того, что поставщик контролирует технологию аутентификации и мониторинга и может распределить потери между всеми клиентами через тарифы, а пользователь отвечает за то, что зависит от него: сохранность кодов и своевременное уведомление. Конкретный размер фиксированной суммы, выраженной в базовых расчетных величинах (БРВ), должен определить законодатель с учетом уровня доходов населения.

Обсуждение. Полученные результаты позволяют выделить три проблемы. Первая – отсутствие в Гражданском кодексе договора об оказании платежных услуг. Платежная организация не открывает банковский счет, но обязуется исполнить распоряжение клиента о переводе денежных средств или электронных денег. Квалификация такого договора как договора возмездного оказания услуг не учитывает, что результатом услуги является исполнение денежного обязательства, а надлежащее исполнение зависит от действий других участников системы. Как показывает Б. Гева, платеж в современной системе представляет собой не передачу вещи, а цепочку взаимосвязанных обязательств посредников [9]. Поэтому обоснованно закрепить в Гражданском кодексе рамочный договор об оказании платежных услуг с отсылкой к нормам о расчетах, если иное не предусмотрено законом. Это согласуется и с выводом Ж. Эрполата о необходимости пересмотра ст. 795 Гражданского кодекса [12].

Вторая проблема касается основания ответственности. Поставщик платежных услуг осуществляет предпринимательскую деятельность и в силу общего правила Гражданского кодекса отвечает за нарушение обязательства независимо от вины, если не докажет, что надлежащее исполнение оказалось невозможным вследствие непреодолимой силы [14]. Правило ст. 37 Закона, по которому до уведомления все риски несет держатель, с этой конструкцией согласуется плохо: оно не различает случаи, когда держатель нарушил правила безопасности, и случаи, когда реквизиты были похищены из систем поставщика или третьих лиц без какого-либо участия держателя. Если же ответственность по законопроекту 2026 г. будет поставлена в зависимость от доказанного пользователем нарушения требований кибербезопасности, специальная норма может на практике сузить защиту по сравнению с общими положениями кодекса. Европейский опыт, подтвержденный решением Суда ЕС по делу C-70/25, свидетельствует в пользу иного решения: поставщик сначала возвращает средства, а затем доказывает умысел или грубую неосторожность клиента [21].

Третья проблема – операции, совершенные самим клиентом под влиянием обмана. Формально такой платеж является санкционированным, поэтому правила о несанкционированных операциях к нему не применяются. Европейский законодатель в PSR

решает этот вопрос через превентивные обязанности поставщика (сверка получателя, обмен информацией о мошенничестве) и ответственность за их неисполнение [13; 20], российский – через обязанность приостанавливать переводы в адрес получателей из базы данных Банка России и возмещать средства при ее нарушении [22]. Для Узбекистана приемлемым представляется сочетание этих подходов: ответственность поставщика наступает, если он не применил предусмотренные законом и правилами платежной системы меры предотвращения мошенничества, а клиент, действовавший с грубой неосторожностью, несет часть убытков.

Следует учитывать и возражения против переноса риска на поставщиков. Расширение их ответственности может повлечь рост тарифов и более строгие ограничения операций, а также ослабить стимулы пользователей к осмотрительности. Поэтому предлагаемая модель предполагает не абсолютную ответственность поставщика, а сочетание его ответственности с фиксированным пределом убытков пользователя и исключениями для умысла и грубой неосторожности. При такой конструкции поставщик, контролирующий технологию, заинтересован в эффективной защите, а пользователь – в соблюдении правил безопасности. Дальнейшие исследования целесообразно направить на анализ судебной практики Узбекистана после вступления в силу законов 2026 г. и на оценку того, как новые правила скажутся на стоимости платежных услуг.

Заключение. Ответы на поставленные вопросы позволяют сформулировать следующие выводы и предложения.

Во-первых, электронная платежная система представляет собой совокупность гражданско-правовых договоров, в которой правила платежной системы выполняют функцию стандартных условий договора присоединения. Отношения поставщика с пользователем нуждаются в самостоятельной договорной конструкции. Предлагается дополнить Гражданский кодекс положениями о договоре об оказании платежных услуг, определив его существенные условия, порядок исполнения распоряжений и распределение рисков.

Во-вторых, электронные деньги и безналичные денежные средства представляют собой обязательственные права требования к эмитенту (банку). Исполнение по распоряжению, не исходящему от управомоченного лица, не прекращает обязательство эмитента, и риск такой операции по общему правилу несет поставщик.

В-третьих, в Закон «О платежах и платежных системах» целесообразно включить единые для всех платежных инструментов правила о несанкционированных платежах, предусмотрев: а) возложение на поставщика бремени доказывания авторизации операции; б) фиксированный предел убытков пользователя, не допустившего умысла или грубой

неосторожности, выраженный в базовых расчетных величинах, вместо правила о несении держателем всех рисков до уведомления; в) возврат средств не позднее следующего рабочего дня после уведомления с правом последующего требования к пользователю; г) освобождение пользователя от убытков, если поставщик не применил многофакторную аутентификацию, предусмотренную ст. 53 Закона.

В-четвертых, при доработке законопроекта 2026 г. о кибербезопасности и противодействии правонарушениям в цифровой среде основание ответственности поставщика целесообразно сформулировать через презумпцию его ответственности, опровергаемую доказательством умысла или грубой неосторожности пользователя, а для переводов, совершенных клиентом под влиянием обмана, – через перечень превентивных мер, неисполнение которых влечет обязанность возместить ущерб. Это обеспечит согласованность специальных норм с общими положениями Гражданского кодекса об ответственности лиц, осуществляющих предпринимательскую деятельность.

Список литературы:

1. Указ Президента Республики Узбекистан от 5 октября 2020 г. № УП-6079 «Об утверждении Стратегии «Цифровой Узбекистан – 2030» и мерах по ее эффективной реализации» // Национальная база данных законодательства. – URL: https://lex.uz/docs/5031048

2. Cashless transactions surge as bank card usage rises across Uzbekistan // Kun.uz. – 09.02.2026. – URL: https://kun.uz/en/news/2026/02/09/cashless-transactions-surge-as-bank-card-usage-rises-across-uzbekistan

3. KPMG в Узбекистане. Обзор платежных организаций Узбекистана (по заказу Центрального банка Республики Узбекистан). – Ташкент, 2026. – URL: https://kpmg.com/uz/ru/insights/2026/09/overview-of-payment-organizations.html

4. Сенат одобрил закон об усилении защиты платежных систем и борьбе с мошенничеством // Anhor.uz. – 08.04.2026. – URL: https://anhor.uz/news/payment-system/

5. Закон о кибербезопасности усиливает защиту граждан и платежей // UzDaily.uz. – 22.07.2026. – URL: https://www.uzdaily.uz/ru/zakon-o-kiberbezopasnosti-usilivaet-zashchitu-grazhdan-i-platezhei/

6. Новоселова Л.А. Денежные расчеты в предпринимательской деятельности. – М.: Статут, 1996.

7. Ефимова Л.Г. Банковские сделки: право и практика. – М.: НИМП, 2001.

8. Белов В.А. Денежные обязательства. – М.: АО «Центр ЮрИнфоР», 2001.

9. Geva B. Bank Collections and Payment Transactions: Comparative Study of Legal Aspects. – Oxford: Oxford University Press, 2001.

10. AllahRakha N. Legal Analysis of the Law of the Republic of Uzbekistan “On Payments and Payment System” // TSUL Legal Report. – 2024. – Vol. 5, № 1. – P. 38–55. – URL: https://legalreport.tsul.uz/index.php/legalreport/article/view/53

11. Tukhtaev U. Issues of Regulating Electronic Payments in the Republic of Uzbekistan // Oriental Renaissance: Innovative, Educational, Natural and Social Sciences. – 2024. – P. 448–454. – URL: https://oriens.uz/en/journal/article/issues-of-regulating-electronic-payments-in-the-republic-of-uzbekistan/

12. Erpolat Zh. Civil Liability for Failure to Fulfill Obligations in the Provision of Payment Services // European and Asian Law Review. – 2025. – Vol. 8, № 2. – P. 65–72. – URL: https://ealawreview.3nv.ru/index.php/ea/article/view/206

13. Van Praag E., Steenot R., Kjorven M.E., Omland L.P.H., Guimarães M.R., Jansen K., Breukelaar S., Fejős A. Authorized Push Payment Fraud: Suggestions for the Draft Payment Services Regulation // European Review of Private Law. – 2025. – Vol. 33, № 5–6. – P. 1039–1072. – DOI: 10.54648/erpl2025066

14. Гражданский кодекс Республики Узбекистан (часть первая – утв. Законом от 21.12.1995 № 163-I; часть вторая – утв. Законом от 29.08.1996 № 256-I) // Национальная база данных законодательства. – URL: https://lex.uz/docs/111181

15. Закон Республики Узбекистан от 1 ноября 2019 г. № ЗРУ-578 «О платежах и платежных системах» (с изм. и доп.) // Национальная база данных законодательства. – URL: https://lex.uz/docs/4575788

16. Федеральный закон Российской Федерации от 27 июня 2011 г. № 161-ФЗ «О национальной платежной системе» // Собрание законодательства РФ. – 2011. – № 27. – Ст. 3872.

17. Закон Республики Казахстан от 26 июля 2016 г. № 11-VI «О платежах и платежных системах» // Информационно-правовая система «Әділет». – URL: https://adilet.zan.kz/rus/docs/Z1600000011

18. Directive (EU) 2015/2366 of the European Parliament and of the Council of 25 November 2015 on payment services in the internal market // Official Journal of the European Union. – L 337. – 23.12.2015. – P. 35–127.

19. Directive 2009/110/EC of the European Parliament and of the Council of 16 September 2009 on the taking up, pursuit and prudential supervision of the business of electronic money institutions // Official Journal of the European Union. – L 267. – 10.10.2009. – P. 7–17.

20. Council of the European Union. Payment services: Council and Parliament agree to step up the fight against fraud and increase transparency. Press release № 1001/25. – Brussels, 27.11.2025. – URL: https://www.consilium.europa.eu/en/press/press-releases/

21. Judgment of the Court of Justice of the European Union (First Chamber) of 15 October 2026, Case C-70/25 (Tukowiecka). – ECLI:EU:C:2026:852. – URL: https://curia.europa.eu/juris/liste.jsf?num=C-70/25

22. Федеральный закон Российской Федерации от 24 июля 2023 г. № 369-ФЗ «О внесении изменений в Федеральный закон «О национальной платежной системе» и отдельные законодательные акты Российской Федерации» // Официальный интернет-портал правовой информации. – URL: http://pravo.gov.ru

23. Блокировка счетов казахстанцев: в Нацбанке рассказали о новых поправках // Tengrinews.kz. – 28.08.2025. – URL: https://tengrinews.kz/kazakhstan_news/blokirovka-schetov-kazahstantsev-natsbanke-rasskazali-novyih-579235/